

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2005 年 7 月 21 日 (21.07.2005)

PCT

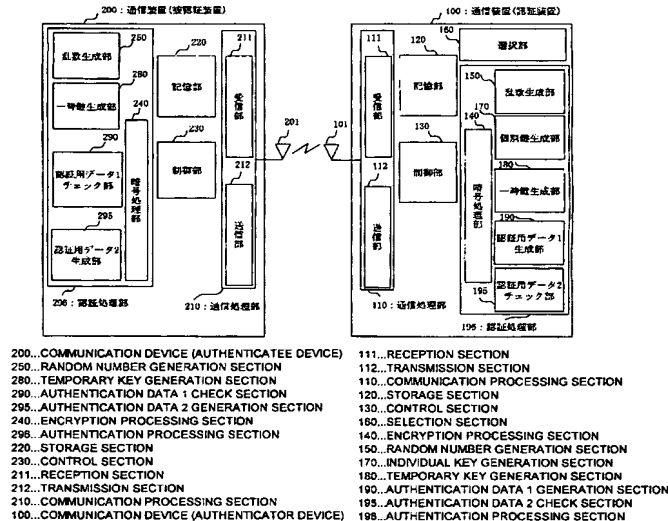
(10) 国際公開番号
WO 2005/067199 A1

- (51) 国際特許分類: H04L 9/14, 9/32
- (21) 国際出願番号: PCT/JP2004/005881
- (22) 国際出願日: 2004 年 4 月 23 日 (23.04.2004)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2003-432476
2003 年 12 月 26 日 (26.12.2003) JP
- (71) 出願人 (米国を除く全ての指定国について): 三菱電機株式会社 (MITSUBISHI DENKI KABUSHIKI KAISHA) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目 2 番 3 号 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 大越 丈弘 (OHKOSHI, Takehiro) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目 2 番 3 号 三菱電機株式会社内 Tokyo (JP). 山田 敬喜 (YAMADA, Keiki) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目 2 番 3 号 三菱電機株式会社内 Tokyo (JP). 牧田 覚 (MAKITA, Satoru) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目 2 番 3 号 三菱電機株式会社内 Tokyo (JP).
- (74) 代理人: 溝井 章司 (MIZOI, Shoji); 〒2470056 神奈川県鎌倉市大船二丁目 17 番 10 号 NTA 大船ビル 3 階 溝井国際特許事務所 Kanagawa (JP).
- (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM,

[続葉有]

(54) Title: AUTHENTICATEE DEVICE, AUTHENTICATOR DEVICE, AND AUTHENTICATION METHOD

(54) 発明の名称: 被認証装置及び認証装置及び認証方法



(57) Abstract: An authenticatee device (200) includes: a storage section (220) for storing at least one algorithm identifier and at least one encryption key identifier; a transmission section (212) for transmitting the at least one algorithm identifier and the at least one encryption key identifier stored in the storage section (220) to an authenticator device (100); a reception section (211) for receiving a predetermined algorithm identifier and a predetermined encryption key identifier selected from the at least one algorithm identifier and the at least one encryption key identifier transmitted from the authenticator device (100) by the transmission section (212); and an authentication processing section (296) for performing authentication processing together with the authenticator device (100) according to the predetermined algorithm identifier and the encryption key identifier received by the reception section (211).

(57) 要約: 被認証装置 200 に、少なくとも 1 つのアルゴリズム識別子と少なくとも 1 つの暗号鍵識別子とを記憶する記憶部 220 と、上記記憶部 220 により記憶された少なくとも 1 つのアルゴリズム識別子と少なくとも 1 つの暗号鍵識別子とを認証装置 100 に送信する送信部 212 と、上記認証装置 100 から上記送信部 212 により送信された少なくとも 1 つのアルゴリズム識別子と少なくとも 1 つの暗号鍵識別子とを受信する受信部 211 と、上記受信部 211 により受信された少なくとも 1 つのアルゴリズム識別子と少なくとも 1 つの暗号鍵識別子とを用いて認証処理を行う認証処理部 296 とを備える。

[続葉有]



DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告書

- (84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY,

2 文字コード及び他の略語については、定期発行される各 PCT ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

BEST AVAILABLE COPY